the manufacture, sale, use, or operation of anti-terrorism technology for which a Designation is issued (regardless of whether such contract is entered into before or after the issuance of such Designation), including, without limitation, an independent laboratory or other entity engaged in testing or verifying the safety, utility, performance, or effectiveness of such technology, or the conformity of such technology to the Seller's specifications.

Designation—The term "Designation" means a designation of a qualified anti-terrorism technology under the SAFETY Act issued by the Under Secretary under authority delegated by the Secretary of Homeland Security.

Loss—The term "loss" means death, bodily injury, or loss of or damage to property, including business interruption loss (which is a component of loss of or damage to property).

Noneconomic damages—The term "noneconomic damages" means damages for losses for physical and emotional pain, suffering, inconvenience, physical impairment, mental anguish, disfigurement, loss of enjoyment of life, loss of society and companionship, loss of consortium, hedonic damages, injury to reputation, and any other nonpecuniary losses.

Physical harm—The term "physical harm" as used in the Act shall mean a physical injury to the body that caused, either temporarily or permanently, partial or total physical disability, incapacity or disfigurement. In no event shall physical harm include mental pain, anguish, or suffering, or fear of injury.

Qualified Anti-Terrorism Technology (QATT)—The term "'qualified anti-terrorism technology"' means any product, equipment, service (including support services), device, or technology (including information technology) designed, developed, modified, or procured for the specific purpose of preventing, detecting, identifying, or deterring acts of terrorism or limiting the harm such acts might otherwise cause, for which a Designation has been issued under this Part.

SAFETY Act or Act—The term "SAFETY Act" or "Act" means the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, enacted as Subtitle G of Title VIII of the Homeland Security Act of 2002, Public Law 107–296.

Seller—The term "Seller" means any person or entity to whom or to which (as appropriate) a Designation has been issued under this Part (unless the context requires otherwise).

Under Secretary—The term "Under Secretary" means the Under Secretary for Science and Technology of the Department of Homeland Security.

PART 29—PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Sec.

AUTHORITY: Pub. L. 107–296, 116 Stat. 2135 (6 U.S.C. 1 *et seq.*); 5 U.S.C. 301.

SOURCE: 69 FR 8083, Feb. 20, 2004, unless otherwise noted.

§ 29.1 Purpose and scope.

(a) *Purpose of the rule.* This part implements section 214 of Title II, Subtitle B, of the Homeland Security Act of 2002 through the establishment of uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal government through the Department of Homeland Security. Title II, Subtitle B, of the Homeland Security Act is referred to herein as the Critical Infrastructure Information Act of 2002 (CII Act of 2002). Consistent with the statutory mission of the Department of Homeland Security (DHS) to prevent terrorist attacks within the United States and reduce the vulnerability of the United States to terrorism, it is the policy of DHS to encourage the voluntary submission of CII by safeguarding and protecting that information from unauthorized disclosure and

by ensuring that such information is expeditiously and securely shared with appropriate authorities including Federal national security, homeland security, and law enforcement entities and, consistent with the CII Act of 2002, with State and local officials, where doing so may reasonably be expected to assist in preventing, preempting, and disrupting terrorist threats to our homeland. As required by the CII Act of 2002, the procedures established herein include mechanisms regarding:

(1) The acknowledgement of receipt by DHS of voluntarily submitted CII;

(2) The maintenance of the identification of CII voluntarily submitted to DHS for purposes of, and subject to the provisions of the CII Act of 2002;

(3) The receipt, handling, storage, and proper marking of information as Protected CII;

(4) The safeguarding and maintenance of the confidentiality of such information that permits the sharing of such information within the Federal government and with foreign, State, and local governments and government authorities, and the private sector or the general public, in the form of advisories or warnings; and

(5) The issuance of notices and warnings related to the protection of critical infrastructure and protected systems in such a manner as to protect from unauthorized disclosure the identity of the submitting person or entity as well as information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily available in the public domain.

(b) *Scope.* These procedures apply to all Federal agencies that handle, use, or store Protected CII pursuant to the CII Act of 2002. In addition, these procedures apply to United States Government contractors, to foreign, State, and local governments, and to government authorities, pursuant to any necessary express written agreements, treaties, bilateral agreements, or other statutory authority.

§ 29.2 Definitions.

For purposes of this part:

Critical Infrastructure has the definition referenced in section 2 of the Homeland Security Act of 2002 and means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Critical Infrastructure Information, or CII means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. CII consists of records and information concerning:

(1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms the interstate commerce of the United States, or threatens public health or safety;

(2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk-management planning, or risk audit; or

(3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

Critical Infrastructure Information Program, or CII Program means the maintenance, management, and review of these procedures and of the information provided to DHS in furtherance of the protections provided by the CII Act of 2002.

Information Sharing and Analysis Organization, or ISAO means any formal or informal entity or collaboration created or employed by public or private sector organizations for purposes of:

(1) Gathering and analyzing CII in order to better understand security